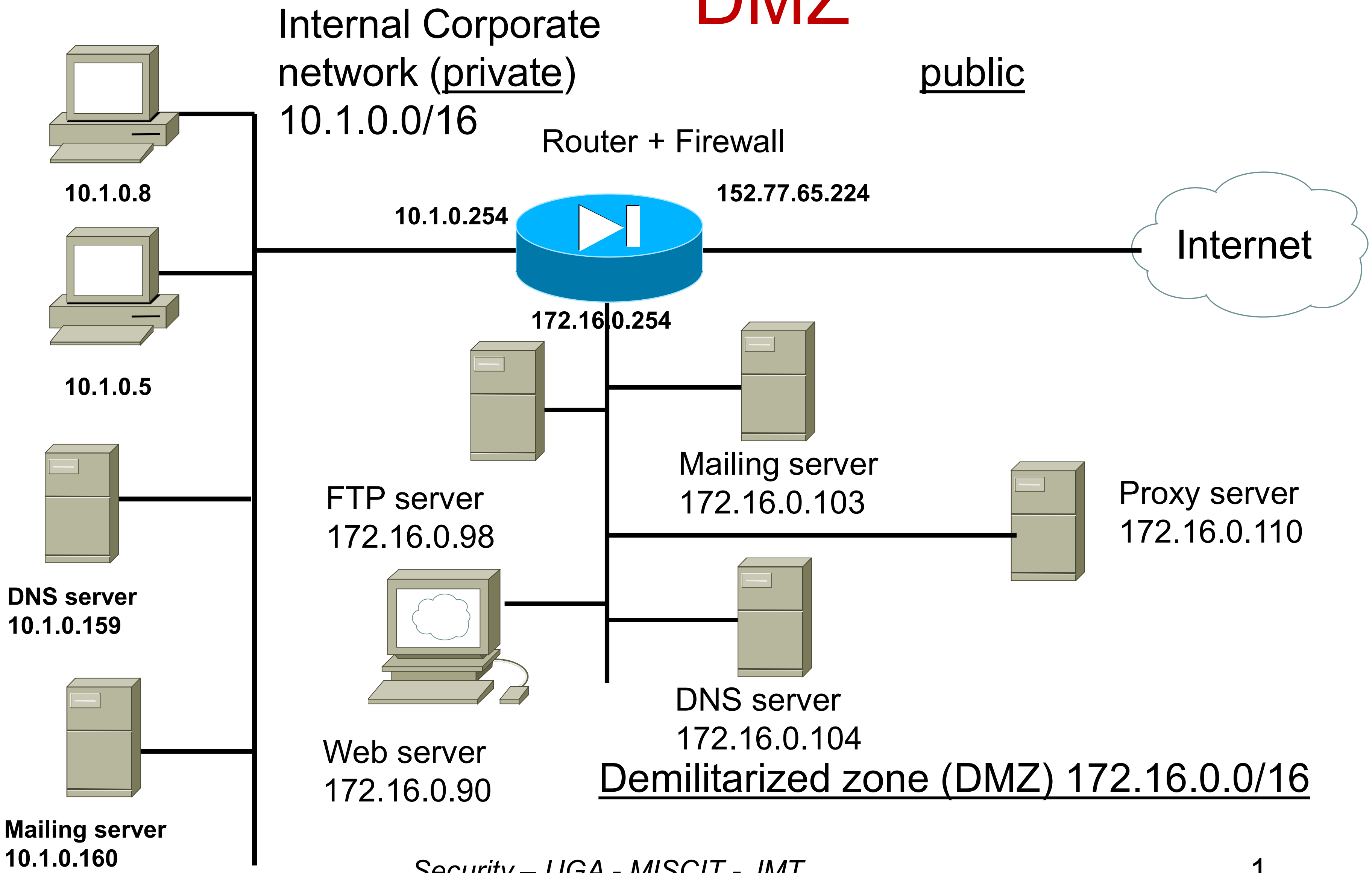
A network with a firewall/router…



Exercise 1

- We use a stateful firewall
- The machines from the inside network should be able to reach any machine in the DMZ or outside (for the mail)
  - Access-list 1 permit mail 10.1.0.0/16 any eq 25
- The machines from the DMZ should be able to reach any machine in outside BUT NOT inside (for the mail)
  - Access-list 1 deny mail 172.16.0.0/16 10.1.0.0/16 eq 25 (should be before !)
  - Access-list 1 permit mail 172.16.0.0/16 any eq 25
- Concerning http
  - Any machine from inside should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
  - Access-list 1 permit tcp/udp 10.1.0.0/16 172.16.0.110 eq 3128
  - Any machine from the DMZ should NOT reach directly an http somewhere, but the request should be sent to the proxy machine (using the 3128 port)
  - No rule
  - The proxy should be able to reach any http server (port 80) everywhere
  - Access-list 1 permit tcp 172.16.0.110 any eq 80
- We should not forget the DNS aspects (port 53)
  - Access-list 1 permit tcp/udp 10.1.0.159 172.16.0.104 eq 53
  - Access-list 1 permit tcp/udp 172.16.0.104 a_specific_DNS_Server_outside eq 53
  - Access-list 1 deny any any any eq any

Exercise 2

- Let’s consider an architecture around a stateful firewall
- We wish to set up :
  1. All the machines of the internal network must ping the DMZ or the outside.
  2. All the machines in the DMZ must be able to ping outside but not on the internal network.
  3. All the machines from the inside must be able to reach http or https servers through the proxy.
  4. The DNS server of the internal network must be able to reach the DNS of the DMZ on port 53.
  5. The DNS server of the DMZ must be able to reach an external DNS (IP: 143.210.47.211).
- Actions to be carried out If necessary,
  - set up translation rules
  - Write filter rules and comment on them
- Audit of our security strategy
  - All the machines in the internal network have to be connected to the DMZ or to the outside. Is this a good strategy? Why is it a good strategy?
  - All the machines in the DMZ must ping the outside but not the internal network. Why this strategy?

Translation rules

- They are necessary because we use private addresses.
- 10.1.0.0/16 any 152.77.65.224; machines on the internal network exit to the public network using the unique public address 152.77.65.224
- 172.16.0.0/16 any 152.77.65.224; DMZ machines exit to the public network using the unique public address 152.77.65.224

Filtering rules

Protocol	Source	Destination	Service (port number)	Action	Comment
ICMP	10.1.0.0/16	Any	Any	Pass	Internal network ping everywhere
ICMP	172.16.0.0/16	10.1.0.0/16	Any	Block	No pings from DMZ to internal network
ICMP	172.16.0.0/16	Any	Any	Pass	DMZ ping everywhere
TCP	10.1.0.0/16	172.16.0.110	Httpproxy	Pass	TCP traffic from internal network to proxy
TCP	172.16.0.110	Any	http, https	Pass	TCP traffic from proxy to http servers everywhere
TCP,UDP	10.1.0.159	172.16.0.104	Dns (port 53)	Pass	DNS from internal network to DMZ
TCP,UDP	172.16.0.104	143.210.47.211	Dns (port 53)	Pass	DNS from DMZ to external DNS

Some considerations about NAT

Network Address Translation

NAT function (network address translation)

- Internet Addresses (IPv4)
  - Theory, 2^{32} addresses (~4,3.10^9 addresses)
  - Practical
    - Public addresses: ~3,2.10^9
    - Reserved addresses: test…
    - Private addresses: reserved for the internal networks (non accessible from outside)
      - 10.0.0.0 to 10.255.255.255 (prefix 10/8)
      - 172.16.0.0 to 172.31.255.255 (prefix 172.16/12)
      - 192.168.0.0 to 192.168.255.255 (prefix 192.168/16)
- NAT ensures the conversion between public and private addresses, between the internal network and the outside accesses
  - firewall,
  - sometimes a router or a computer